

WHAT IS CLAIMED IS:

1. An integrated circuit comprising:
 - (a) a processor for:
 - (i) requesting encrypted digital data, and
 - (ii) decrypting the encrypted digital data, thereby providing decrypted digital data; and
 - (b) a player for transforming said decrypted digital data to analog signals.
2. The integrated circuit of claim 1, wherein said encrypted digital data is requested from a server and wherein said requesting of said encrypted digital data includes authenticating the integrated circuit to said server.
3. The integrated circuit of claim 1, wherein the integrated circuit is tamper-resistant.
4. The integrated circuit of claim 1, wherein said encrypted digital data are audio data.
5. The integrated circuit of claim 1, wherein said encrypted digital data are video data.
6. The integrated circuit of claim 1, wherein said processor includes an interface for receiving said encrypted digital data.

7. The integrated circuit of claim 6, wherein said interface is selected from the group consisting of an ISO7816 interface, a local bus interface, a MMCA interface, a SDA interface, a USB interface and a parallel interface.

8. The integrated circuit of claim 1, having a form factor selected from the group consisting of a SIM form factor, a TQFP form factor, a DIP form factor, a SOP form factor and a BGA form factor.

9. A device for receiving, decrypting and displaying said encrypted digital data, comprising the integrated circuit of claim 1.

10. The device of claim 9, further comprising a transceiver for transmitting a request for said encrypted digital data from said processor and for receiving said encrypted digital data.

11. The device of claim 9, further comprising a display mechanism for displaying said analog signals.

12. The device of claim 9, further comprising a non-volatile memory for storing said encrypted digital data.

13. The device of claim 12, wherein said non-volatile memory is a flash memory.

14. The integrated circuit of claim 1, comprising a single said processor.

15. The integrated circuit of claim 1, further comprising:
 - (c) a ROM for storing management code that is executed by said processor to operate the integrated circuit.
16. The integrated circuit of claim 15, wherein said management code is stored only in said ROM.
17. A system for displaying digital data, comprising:
 - (a) a server for storing the digital data in an encrypted form; and
 - (b) a user platform including:
 - (i) an integrated circuit that includes:
 - (A) a processor for:
 - (I) requesting said encrypted digital data from said server, and
 - (II) decrypting said encrypted digital data, thereby providing decrypted digital data, and
 - (B) a player for transforming said decrypted digital data to analog signals.
18. The system of claim 17, wherein said requesting of said encrypted digital data from said server includes authenticating said integrated circuit to said server.
19. The system of claim 17, wherein said integrated circuit is tamper resistant.

20. The system of claim 17, wherein said user platform further includes:
- (ii) a transceiver for transmitting to said server a request for said encrypted digital data and for receiving said encrypted digital data.
21. The system of claim 17, wherein said user platform further includes:
- (ii) a display mechanism for displaying said analog signals.
22. The system of claim 17, wherein said user platform further includes:
- (ii) a non-volatile memory for storing said encrypted digital data.
23. The system of claim 22, wherein said non-volatile memory is a flash memory.
24. The system of claim 17, wherein said integrated circuit includes a single said processor.
25. The system of claim 17, wherein said server is configured to transmit substantially only said encrypted digital data to said user platform.
26. The system of claim 17, wherein said integrated circuit further includes:
- (C) a ROM for storing management code that is executed by said processor to operate said integrated circuit.

27. The system of claim 26, wherein said management code is stored only in said ROM.

28. A method of requesting encrypted digital data from a server and then decrypting and displaying the encrypted digital data, comprising the steps of:

- (a) providing an integrated circuit that includes:
 - (i) a processor operative to:
 - (A) request the encrypted digital data from the server and
 - (B) decrypt the encrypted digital data, thereby providing decrypted digital data, and
 - (ii) a player operative to transform said decrypted digital data to analog signals;
- (b) requesting the encrypted digital data from the server, by said processor;
- (c) decrypting the encrypted digital data, by said processor, thereby providing said decrypted digital data; and
- (d) transforming said decrypted digital data to analog signals, by said player.

29. The method of claim 28, wherein said requesting includes authenticating said integrated circuit to the server.

30. The method of claim 29, wherein said authenticating is effected using an asymmetrical algorithm.

31. The method of claim 30, wherein said asymmetrical algorithm is a RSA algorithm.

32. The method of claim 30, wherein said asymmetrical algorithm is a ECC algorithm.

33. The method of claim 28, wherein said decrypting is effected using a symmetrical algorithm.

34. The method of claim 33, wherein said symmetrical algorithm is a DES algorithm.

35. The method of claim 33, wherein said symmetrical algorithm is a Rijndael algorithm.

36. The method of claim 28, wherein said decrypting is effected using at least one key, and wherein the method further comprises the step of:

(e) requesting said at least one key from the server, by said processor.

37. The method of claim 36, wherein the method further comprises the step of:

(f) storing said at least one key in a nonvolatile memory.

38. The method of claim 37, further comprising the step of:
- (g) encrypting said at least one key, prior to said storing of said at least one key in said nonvolatile memory.
39. The method of claim 36, further comprising the step of:
- (f) configuring the server to send substantially only said encrypted digital data and said at least one key to said integrated circuit.
40. The method of claim 28, wherein the method further comprises the step of:
- (e) storing said encrypted digital data in a nonvolatile memory.
41. The method of claim 28, further comprising the step of:
- (e) upon detecting an attempt to tamper with said integrated circuit: resetting said integrated circuit.
42. The method of claim 28, further comprising the step of:
- (e) configuring the server to send substantially only said encrypted digital data to said integrated circuit.